Key Extraction
for Host-Migrated Cable Modem

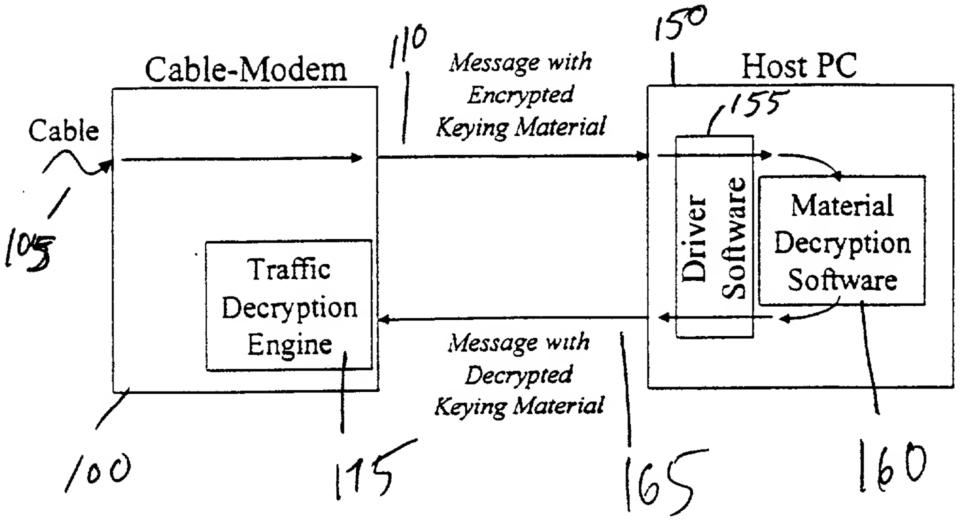
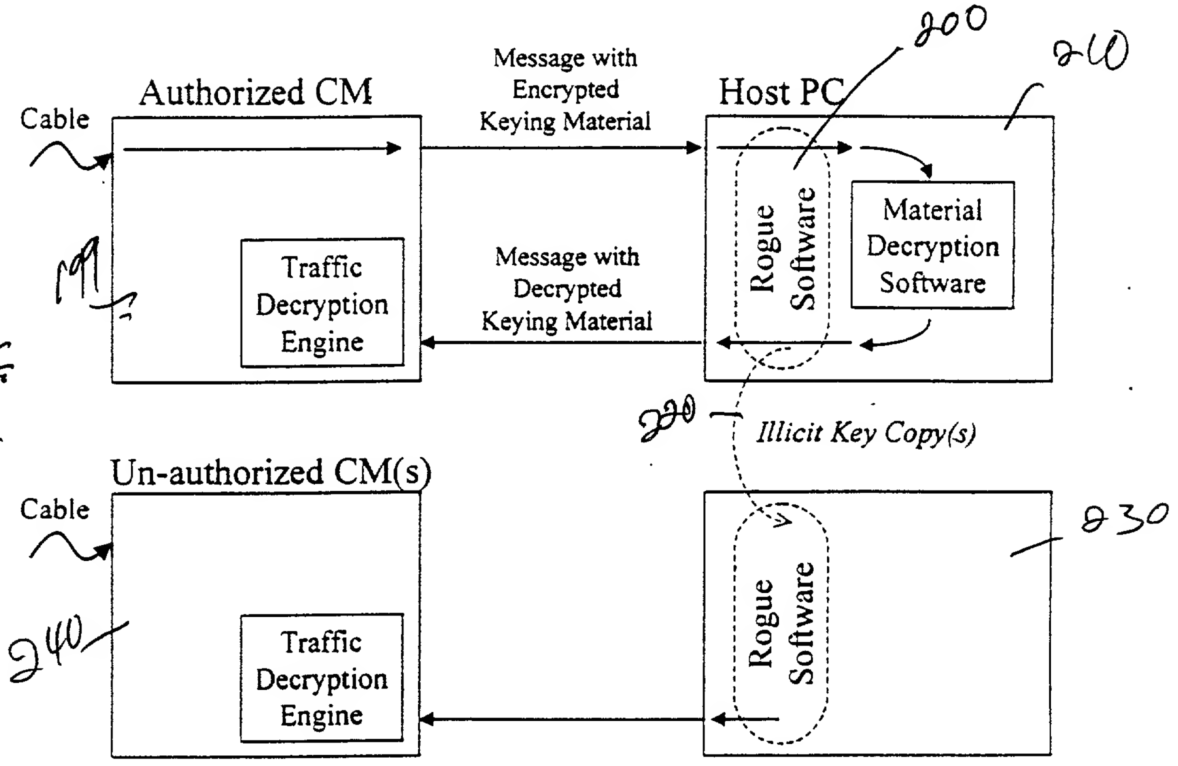

Cable-Modem
Cable
105
110
Message with Encrypted Keying Material
150
Host PC
155
Driver Software
Material Decryption Software
Traffic Decryption Engine
Message with Decrypted Keying Material
100
115
165
160

Fig. 1

Security Threat to Key Extraction on Host-Migrated Cable Modem



200
210
Authorized CM
Cable
Message with Encrypted Keying Material
Host PC
Rogue Software
Material Decryption Software
199
Traffic Decryption Engine
Message with Decrypted Keying Material
220
Illicit Key Copy(s)
Un-authorized CM(s)
Cable
230
Rogue Software
240
Traffic Decryption Engine

FIG 2

Decryption Key handling in CCCM MAC chip

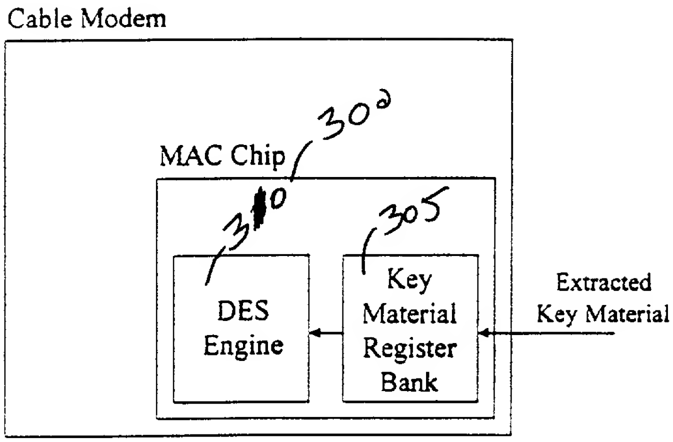


FIG 3

Key Material Register Bank in CM Media Access Controller (MAC) Chip

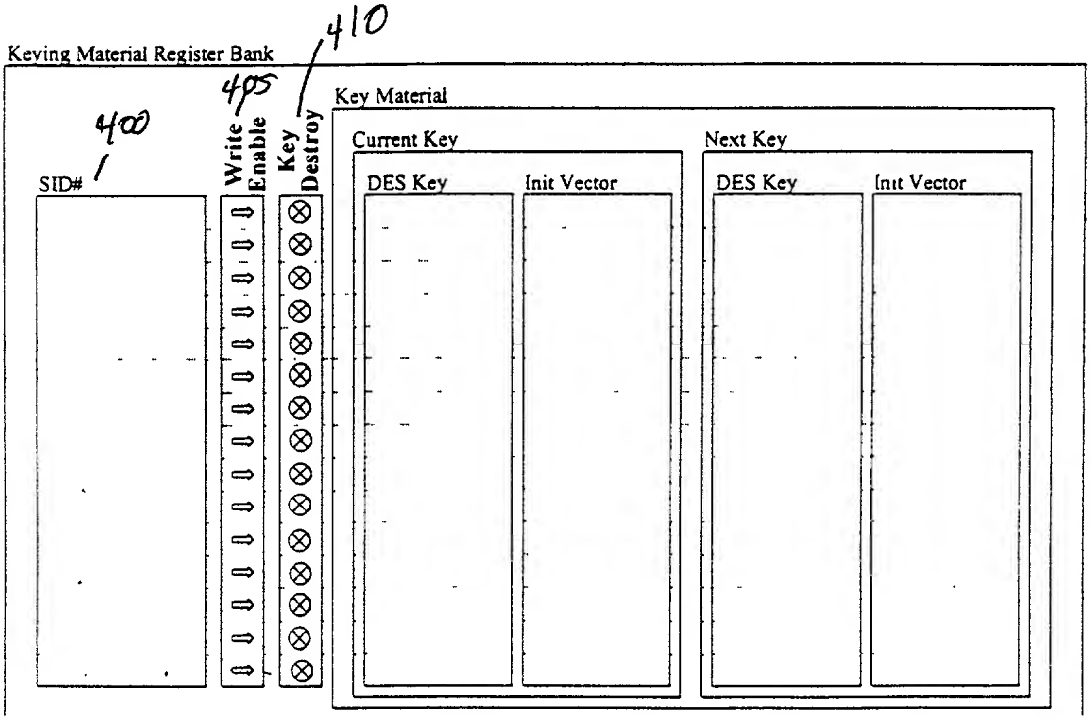
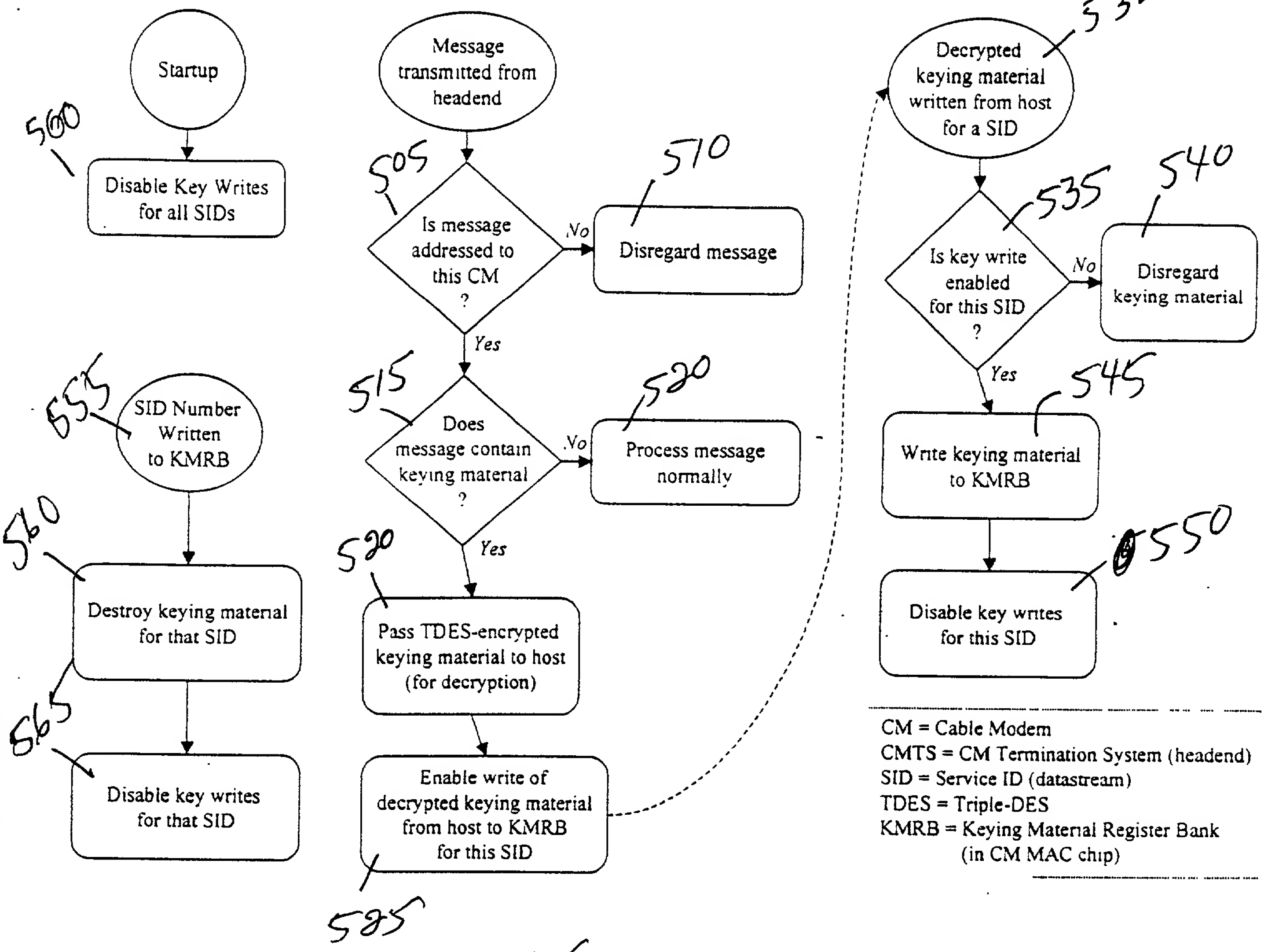


FIG 4

Rules Flow-Chart


Startup
560
Disable Key Writes for all SIDs
Message transmitted from headend
505
Is message addressed to this CM ?
No
510
Disregard message
Yes
515
Does message contain keying material ?
No
520
Process message normally
Yes
520
Pass TDES-encrypted keying material to host (for decryption)
Enable write of decrypted keying material from host to KMRB for this SID
525
555
SID Number Written to KMRB
560
Destroy keying material for that SID
565
Disable key writes for that SID
530
Decrypted keying material written from host for a SID
535
Is key write enabled for this SID ?
No
540
Disregard keying material
Yes
545
Write keying material to KMRB
550
Disable key writes for this SID

CM = Cable Modem
CMTS = CM Termination System (headend)
SID = Service ID (datastream)
TDES = Triple-DES
KMRB = Keying Material Register Bank
(in CM MAC chip)

FIG 5

Generalized Protection case

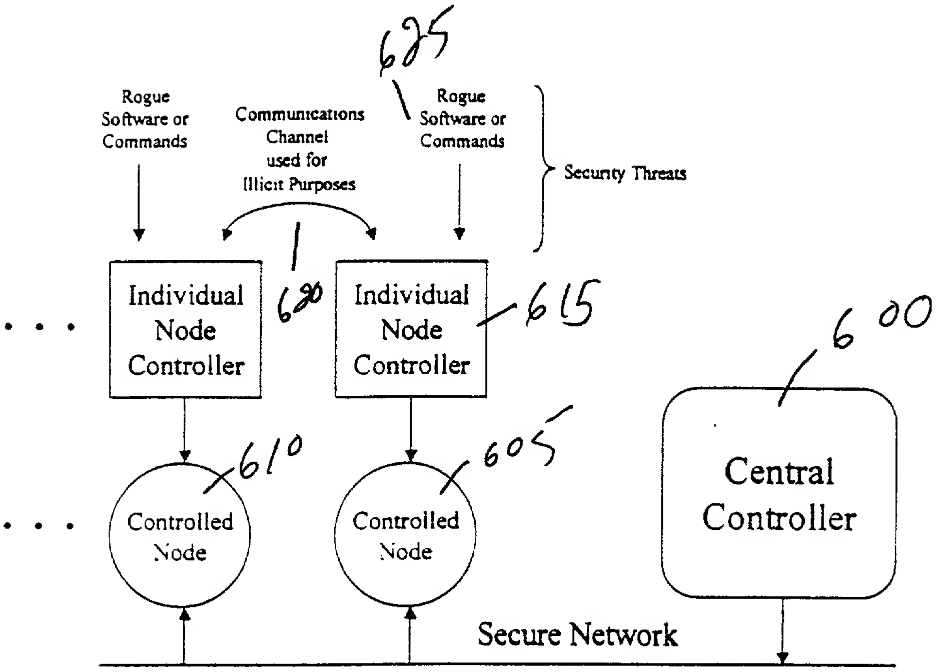


FIG 6